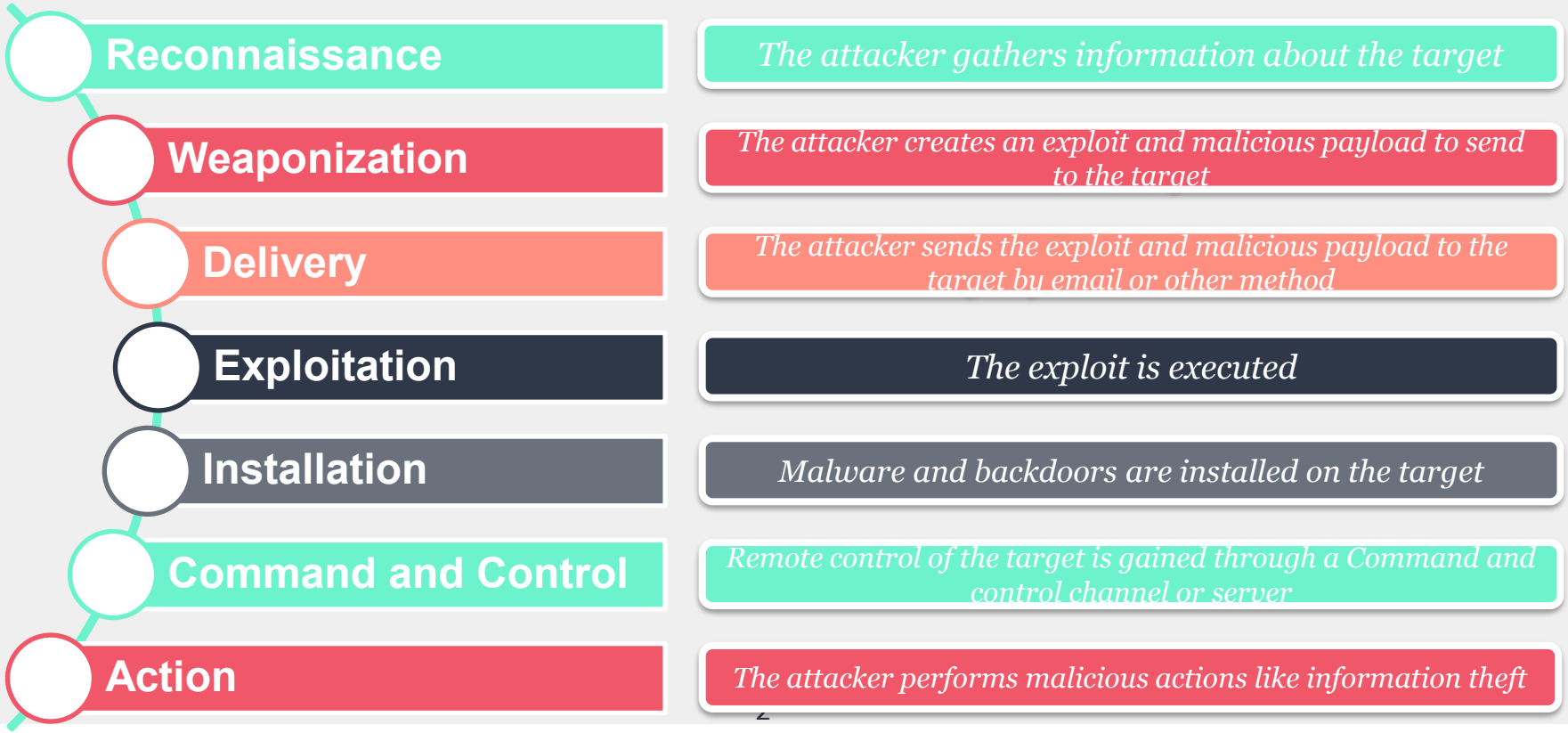
SYSTEM SECURITY

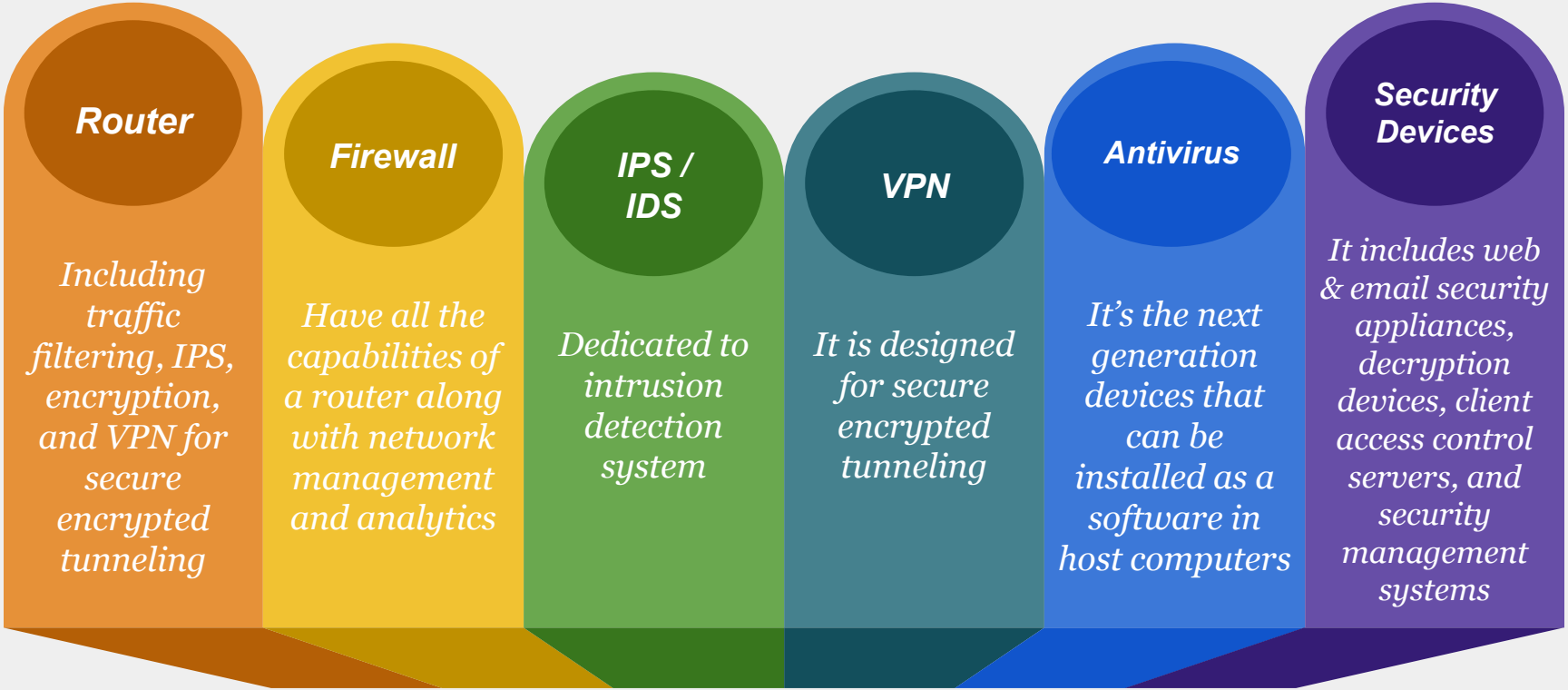
UNIT 2: DESIGN PRINCPLES

By Prof. Krishna Samdani

KILL CHAIN IN CYBER SECURITY



SECURITY APPLIANCES



VARIOUS SECURITY ATTACKS

METHODS OF DEFENSE

- ***Prevent it***: by blocking the attack or closing the vulnerability
- ***Deter it***: making the attack harder but not impossible
- ***Deflect it***: making another target more attractive
- ***Detect it***: either as it happens or after the attack
- ***Recover*** from its effects

NIST SP 800-35 SECURITY LIFE CYCLE

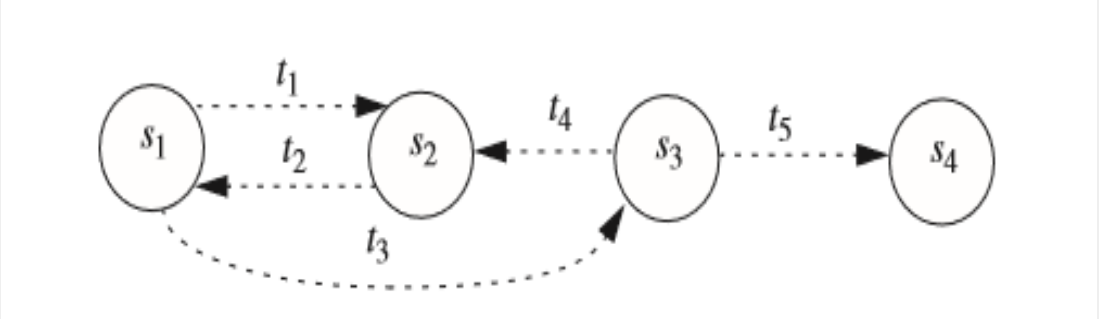
- ***Phase 1: Initiation :*** At this point the organisation is looking into implementing some IT security service, device, or process.
- ***Phase 2: Assessment :*** This phase involves determining and describing the organization's current security posture. It is recommended that this phase use quantifiable metrics.
- ***Phase 3: Solution :*** This is where various solutions are evaluated and one or more are selected.
- ***Phase 4: Implementation :*** In this phase the IT security service, device, or process is implemented.
- ***Phase 5: Operations :*** Phase 5 is the ongoing operation and maintenance of the security service, device, or process that was implemented in phase 4.
- ***Phase 6: Closeout :*** At some point, whatever was implemented in phase 4 will be concluded. Often this is when a system is replaced by a newer and better system

SECURITY POLICIES

- Consider a computer system to be a finite-state automaton with a set of transition functions that change state. Then : ***A security policy is a statement that partitions the states of the system into a set of authorized, or secure, states and a set of unauthorized, or non-secure, states.***

- A security policy sets the context in which we can define a secure system. What is secure under one policy may not be secure under a different policy. More precisely: ***A secure system is a system that starts in an authorized state and cannot enter an unauthorized state.***

SECURITY POLICIES AND TYPES



- Consider the finite-state machine in Figure .
- It consists of four states and five transitions.
- The security policy partitions the states into a set of authorized states A = { s1, s2 } and a set of unauthorized states UA = { s3, s4 }.
- This system is not secure, because regardless of which authorized state it starts in, it can enter an unauthorized state.
- However, if the edge from s1 to s3 were not present, the system would be secure, because it could not enter an unauthorized state from an authorized state.

SECURITY POLICY DEVELOPMENT

One useful approach is to focus on the ***why***, ***who***, ***where***, and ***what*** during the policy development process

- ***Purpose*** – what the policy should address
- ***Responsibility*** – who should the policy address
- ***Scope*** – where the policy be applied
- ***Content*** – what should the policy contain

POLICY CATEGORY

- ***Regulatory*** – for audit and compliance purpose
- ***Advisory*** – generally based on security best practices
- ***Informative*** – which are not included in regulatory or advisory

SECURITY POLICY FORMAT

1. ***Author*** - The policy writer
2. ***Sponsor*** - The Executive champion
3. ***Authorizer*** - The Executive signer with ultimate authority
4. ***Effective date*** - When the policy is effective; generally when authorized
5. ***Review date*** - Subject to agreement by all parties; annually at least
6. ***Purpose*** - Why the policy exists; regulatory, advisory, or informative
7. ***Scope*** - Who the policy affects and where the policy is applied
8. ***Policy*** - What the policy is about
9. ***Exceptions*** - Who or what is not covered by the policy
10. ***Enforcements*** - How the policy will be enforced, and consequences for not following it
11. ***Definitions*** - Terms the reader may need to know
12. ***References*** - Links to other related policies and corporate documents

TYPES OF SECURITY POLICIES

- A ***military security policy*** (also called a government security policy) is a security policy developed primarily to provide confidentiality.
- A ***commercial security policy*** is a security policy developed primarily to provide integrity.
- A ***confidentiality policy*** is a security policy dealing only with confidentiality.
- An ***integrity policy*** is a security policy dealing only with integrity.

DESIGN PRINCIPLES OF SECURITY MECHANISM

- Principle of least privilege
- Principle of Fail-Safe Defaults
- Principle of Economy of Mechanism
- Principle of Complete Mediation
- Principle of Open Design
- Principle of Separation of privilege
- Principle of least common mechanism
- Principle of Psychological acceptability

PRINCIPLE OF LEAST PRIVILEGE

- Restricts how privileges are granted.
- Principle states that "*a subject should be given only those privilege that it needs in order to complete its task.*"
- If a specific action requires that a subject's access rights be augmented, those extra rights be relinquished immediately on completion of the action.

PRINCIPLE OF FAIL-SAFE DEFAULTS

- Restricts how privileges are initialized when a subject or object is created.
- *"The principle of Fail-Safe defaults states that, unless a subject is given explicit access to an object, it should be denied access to that object"*
- This principle requires that the default access to an object is none.

PRINCIPLE OF ECONOMY OF MECHANISM

- Simplifies the design and implementation of security mechanisms.
- *"The principle of economy of mechanism states that security mechanism should be as simple as possible"*
- If a design and implementations are simple, fewer possibilities exist for errors.

PRINCIPLE OF COMPLETE MEDIATION

- This principle restricts the caching of information, which often leads to simpler implementations of mechanisms.
- *"The principle of complete mediation requires that all accesses to objects be checked to ensure that they are allowed."*
- Whenever a subject attempts to read an object, the OS should mediate the action.
- First, it determines if the subject is allowed to read the object. If so, it provides the resources for the read to occur.
- If the subject tries to read it again, the system should check that the subject is still allowed to read the object.
- Most systems would not make the second check.
- They would cache the results of the first check and base the second access on the cached results.

PRINCIPLE OF OPEN DESIGN

- The principle suggests that complexity does not add security.
- *"The principle of open design states that the security of a mechanism should not depend on the secrecy of its design or implementation".*
- Designers of a program must not depend on secrecy of the details of their design and implementation to ensure security.
- If the strength of the program's security depends on the ignorance of the user, a knowledgeable user can defeat that security mechanism.

PRINCIPLE OF SEPARATION OF PRIVILEGE

- This principle is restrictive because it limits access to system entities
- *"The principle of separation of privilege states that a system should not grant permission based on single condition."*
- Company checks for more than $75,000 must be signed by two officers of the company. If either does not sign, the check is not valid. The two conditions are the signatures of two officers.
- This provides a fine-grained control over the resource as well as additional assurance that the access is authorized.

PRINCIPLE OF LEAST COMMON MECHANISM

- This principle is restrictive because it limits sharing.
- *"The principle of least common mechanism states that mechanisms used to access resources should not be shared."*
- Sharing resources provides a channel along which information can be transmitted, and so such sharing should be minimized.

PRINCIPLE OF PSYCHOLOGICAL ACCEPTABILITY

- This principle recognizes the human element in computer security
- *"The Principle of psychological acceptability states that security mechanism should not make the resource more difficult to access than if the security mechanisms were not present."*
- If security related software is too complicated to configure, system administrators may unintentionally set up software in a non secure manner.
- Security-related user programs must be easy to use and must output understandable messages.

STUDY MATERIALS

- Matt Bishop,“ Introduction to Computer Security ”, Pearson Education,2005.

Please Note : PPT’s are for Reference Only , NOT AS A STUDY MATERIAL

Contact

Krishna Samdani

krishna.samdani@nmims.edu

Mobile- 9920407045

Seating – 1A Faculty Area MPSTME Building

Thanks!

Any questions?